

Configuring Threat Mitigation

To support threat mitigation with the Threat Mitigation Application in an SRC network, configure services that can be activated to act on threats detected by IDP sensors that are managed by NetScreen-Security Manager. We recommend that you activate the services as close as possible to the interfaces where the problem traffic entered the network.

To use the Threat Mitigation Application, perform the following tasks:

- Access the local configuration
- Deploy the application. See [Deploying the Threat Mitigation Application](#)
- Apply services. See [Applying Services to Manage Threats](#).

Also see [Examples: Classifying Subscribers and Interfaces for the Threat Mitigation Application](#).

Some sections provide references to entries in the sample data that demonstrate an implementation.

After performing these tasks, configure the script used by NetScreen-Security Manager to implement the messaging that records attacks and identifies actions that the SRC software should take in response to those attacks.

Related Topics

- [Overview of the Threat Mitigation Application](#)
- [Before You Install the Threat Mitigation Application](#)
- [Installing and Initially Configuring the Threat Mitigation Application](#)
- [Configuring a Database to Store Attack and Response Data](#)
- [Configuring the Threat Mitigation Application](#)

